Hilbert's Tenth Problem for Fixed d and n

William Gasarch*

Abstract

Hilbert's 10th problem, stated in modern terms, is

Find an algorithm that will, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$, determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

Davis, Putnam, Robinson, and Matiyasevich showed that there was no such algorithm. But what if we bound the degree of the polynomial? The number of variables? This paper survey's what is known for these cases.

1 Hilbert's Tenth Problem

In 1900 Hilbert proposed 23 problems for mathematicians to work on over the next 100 years (or longer). The 10th problem, stated in modern terms, is

> Find an algorithm that will, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$, determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

Hilbert probably thought this would inspire much deep number theory. And it did inspire some. However, through the efforts of Davis, Putnam, Robinson [3] and Matiyasevich [8] (see also the book by Matiyasevich [9]) it was shown that there is no such algorithm. That is, they showed that there is a d, n such that the problem of, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ of degree d, does it have a solution in $\mathbb{Z}$, is undecidable.

This raises the obvious question of what happens for *particular* numbers of variables n and degree d. I thought that surely there must be a grid on the web where the d-n-th entry is

- D if the problem for degree $\le d$, and $\le n$ variables is Decidable.
- U if the problem for degree $\le d$, and $\le n$ variables is Undecidable.
- ? if the status of the problem for degree $\le d$, and $\le n$ variables is unknown.

*The University of Maryland at College Park, gasarch@umd.edu

Why was there no such grid? I speculate

1. Logicians worked on proving particular (d, n) are undecidable. They sought solutions in $\mathbb{N}$. By contrast number theorists worked on proving particular (d, n) decidable. They sought solutions in $\mathbb{Z}$. Hence a grid would need to reconcile these two related problems.

2. Logicians and number theorists didn't talk to each other. Websites and books on Hilbert's Tenth problem do not mention any solvable cases of it.

3. There is a real dearth of positive results, so a grid would not be that interesting.

4. The undecidable results often involve rather large values of d, so the grid would be hard to draw.

That last point is correct. A grid would be hard to draw. However, there is still a need for a paper to collect up all that is known and point to open problem.s This article is that paper. None of the results are original.

Notation 1.1.

1. $\mathrm{H10}\mathbb{Z}(d, n)$ is the problem where the degree is $\le d$, the number of variables is $\le n$, and we seek a solution in $\mathbb{Z}$.

2. $\mathrm{H10}\mathbb{N}(d, n)$ is the problem where the degree is $\le d$, the number of variables is $\le n$, and we seek a solution in $\mathbb{N}$.

3. $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{D}$ means that there is an algorithm to decide $\mathrm{H10}\mathbb{Z}$.

4. $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{U}$ means that there is no algorithm to decide $\mathrm{H10}\mathbb{Z}$.

5. Similarly for $\mathrm{H10}\mathbb{N}(d, n)$ equal to D or U.

Lemma 1.2.

1. *For every $x \in \mathbb{N}$, there exists $y_1, y_2, y_3, y_4 \in \mathbb{N}$ such that*

$$x = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

2. *For every $x \in \mathbb{N}$ where x is not of the form $4^a(8b+7)$, there exists $y_1, y_2, y_3 \in \mathbb{N}$ such that*

$$x = y_1^2 + y_2^2 + y_3^2.$$

3. *For every* $x \in \mathbb{N}$ *where* $x \equiv 1 \pmod 4$*, there exists* $y_1, y_2 \equiv 0 \pmod 2$ *and* $y_3 \equiv 1 \pmod 2$*, such that*

$$x = y_1^2 + y_2^2 + y_3^2.$$

Proof. 1) This is Lagrange's 4-square theorem.
2) This is Legendre's 3-square theorem. It is sometimes called the Gauss-Legendre Theorem.
3) Since $x \equiv 1 \pmod 4$, x satisfies the hypothesis of part 2. Hence there exists y_1, y_2, y_3 such that

$$x = y_1^2 + y_2^2 + y_3^2.$$

Take this equation mod 4.

$$1 \equiv y_1^2 + y_2^2 + y_3^2 \pmod 4.$$

It is easy to see that the only parities of y_1, y_2, y_3 that work are for two of them to be even and one of them to be odd.

□

Theorem 1.3.

1. *If* $\mathrm{H10}\mathbb{Z}(2d, 4n) = \mathrm{D}$*, then* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{D}$.
2. *If* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{U}$*, then* $\mathrm{H10}\mathbb{Z}(2d, 4n) = \mathrm{U}$*. This is the contrapositive of part 1.*
3. *If* $\mathrm{H10}\mathbb{Z}(2d, 3n) = \mathrm{D}$*, then* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{D}$.
4. *If* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{U}$*, then* $\mathrm{H10}\mathbb{Z}(2d, 3n) = \mathrm{U}$*. This is the contrapositive of part 3.*
5. *If* $\mathrm{H10}\mathbb{Z}(f(d, n), 2n + 2) = \mathrm{D}$*, then* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{D}$ *where*

$$f(d, n) = \max\{2d, (2n + 3)2^n\}.$$

6. *If* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{U}$*, then* $\mathrm{H10}\mathbb{Z}(f(d, n), 2n + 2) = \mathrm{U}$*. This is the contrapositive of part 5.*

Proof. 1) Assume $\mathrm{H10}\mathbb{Z}(2d, 4n) = \mathrm{D}$. We show that $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{D}$.

Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. We want to know if there is a solution in $\mathbb{N}$.

Let q be the polynomial of degree $2d$ with $4n$ variables that you get if you replace each x_i with $y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i4}^2$ where $y_{i1}, y_{i2}, y_{i3}, y_{i4}$ are 4 new variables.

By Lemma 1.2.1 and the fact that for all $w, x, y, z \in \mathbb{Z}$), $w^2 + x^2 + y^2 + z^2 \geq 0$, we have:

p has a solution in $\mathbb{N}$ iff q has a solution in $\mathbb{Z}$.

Use that $\mathrm{H10}\mathbb{Z}(2d, 4n) = \mathrm{D}$ to determine if q has a solution. Hence $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{D}$.

3) Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. We want to know if there is a solution in $\mathbb{N}$.

Let q be the polynomial of degree $2d$ with $3n$ variables that you get if you replace each x_i with $y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i3}$ where y_{i1}, y_{i2}, y_{i3} are 3 new variables. By Lemma 1.2.3 and the fact that for all $w, x, y \in \mathbb{N}$, $w^2 + x^2 + y^2 + y \geq 0$, we have:

p has a solution in $\mathbb{N}$ iff q has a solution in $\mathbb{Z}$.

Use that $\mathrm{H10}\mathbb{Z}(2d, 3n) = \mathrm{D}$ to determine if q has a solution. Hence $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{D}$.

5) This was proven by Sun [12].

□

Theorem 1.4.

1. *If* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{D}$ *then* $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{D}$.

2. *If* $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{U}$ *then* $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{U}$. *This is the contrapositive of part 1.*

Proof. Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. We want to know if there is a solution in $\mathbb{Z}$. For each $\vec{b} = (b_1, \ldots, b_n) \in \{0, 1\}^n$ let $q_{\vec{b}}(x_1, \ldots, x_n)$ be formed as follows: for every i where $b_i = 1$, replace x_i with $-x_i$. It is easy to see that

p has a solution in $\mathbb{Z}$ iff

$(\exists \vec{b})[q_{\vec{b}}$ has a solution in $\mathbb{N}$].

The result follows. □

In the next section we summarize what is known about $\mathrm{H10}\mathbb{N}(d, n)$.

2 When Is $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{U}$? $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{U}$?

The following theorem has many $\mathrm{H10}\mathbb{N}(a, b) = \mathrm{U}$, all due to Jones [6]. From those we use Theorem 1.3 to obtain several $\mathrm{H10}\mathbb{Z}(c, d) = \mathrm{U}$ results.

Theorem 2.1.

1. $\mathrm{H10}\mathbb{N}(4, 58) = \mathrm{U}$ *hence* $\mathrm{H10}\mathbb{Z}(8, 174) = \mathrm{U}$ *and* $\mathrm{H10}\mathbb{Z}(119 \times 2^{58}), 118) = \mathrm{U}$.

2. $\mathrm{H10}\mathbb{N}(8, 38) = \mathrm{U}$ *hence* $\mathrm{H10}\mathbb{Z}(16, 114) = \mathrm{U}$ *and* $\mathrm{H10}\mathbb{Z}(79 \times 2^{38}), 78) = \mathrm{U}$.

3. $\text{H10}\mathbb{N}(12,32) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(24,96) = \text{U}$*and* $\text{H10}\mathbb{Z}(67\times 2^{32}),66) = \text{U}$.
4. $\text{H10}\mathbb{N}(16,29) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(32,87) = \text{U}$*and* $\text{H10}\mathbb{Z}(61\times 2^{29}),60) = \text{U}$.
5. $\text{H10}\mathbb{N}(20,28) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(40,84) = \text{U}$*and* $\text{H10}\mathbb{Z}(59\times 2^{28}),58) = \text{U}$.
6. $\text{H10}\mathbb{N}(24,26) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(48,78) = \text{U}$*and* $\text{H10}\mathbb{Z}(55\times 2^{26}),54) = \text{U}$.
7. $\text{H10}\mathbb{N}(28,25) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(56,75) = \text{U}$*and* $\text{H10}\mathbb{Z}(53\times 2^{25}),52) = \text{U}$.
8. $\text{H10}\mathbb{N}(36,24) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(72,72) = \text{U}$*and* $\text{H10}\mathbb{Z}(51\times 2^{24}),50) = \text{U}$.
9. $\text{H10}\mathbb{N}(96,21) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(192,63) = \text{U}$*and* $\text{H10}\mathbb{Z}(45\times 2^{21}),44) = \text{U}$.
10. $\text{H10}\mathbb{N}(2668,19) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(5336,57) = \text{U}$*and* $\text{H10}\mathbb{Z}(41\times 2^{19}),40) = \text{U}$.
11. $\text{H10}\mathbb{N}(200000,14) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(400000,42) = \text{U}$*and* $\text{H10}\mathbb{Z}(31\times 2^{14}),30) = \text{U}$.
12. $\text{H10}\mathbb{N}(6.6\times 10^{43},13) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(13.2\times 10^{43}),39) = \text{U}$ *and* $\text{H10}\mathbb{Z}(13.2\times 2^{43}),28) = \text{U}$.
13. $\text{H10}\mathbb{N}(1.3\times 10^{44},12) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(2.6\times 10^{44}),36) = \text{U}$ $\text{H10}\mathbb{Z}(2.6\times 2^{44}),26) = \text{U}$.
14. $\text{H10}\mathbb{N}(4.6\times 10^{44},11) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(9.2\times 10^{44}),33) = \text{U}$ $\text{H10}\mathbb{Z}(9.2\times 2^{44}),24) = \text{U}$.
15. $\text{H10}\mathbb{N}(8.6\times 10^{44},10) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(17.2\times 10^{44}),30) = \text{U}$ $\text{H10}\mathbb{Z}(17.2\times 2^{44}),22) = \text{U}$.
16. $\text{H10}\mathbb{N}(1.6\times 10^{45},9) = \text{U}$ *hence* $\text{H10}\mathbb{Z}(3.2\times 10^{45}),27) = \text{U}$ $\text{H10}\mathbb{Z}(3.2\times 2^{45}),20) = \text{U}$.

3 When is $\text{H10}\mathbb{Z}(d,n) = \text{D}$? When is $\text{H10}\mathbb{Z}(d,n) = \text{D}$?

Theorem 3.1.

1. *For all d,* $\text{H10}\mathbb{Z}(d,1) = \text{D}$. *This is elementary.*
2. *For all d,* $\text{H10}\mathbb{N}(d,1) = \text{D}$. *This is elementary.*
3. *For all n,* $\text{H10}\mathbb{Z}(1,n) = \text{D}$. *This is elementary.*

4. *For all n,* $\mathrm{H10}\mathbb{N}(1,n) = \mathrm{D}$. *This is elementary.*

5. $\mathrm{H10}\mathbb{N}(2,2) = \mathrm{D}$. *This is a difficult result of Lagarias [7].*

6. $\mathrm{H10}\mathbb{Z}(2,2) = \mathrm{D}$. *This follows from* $\mathrm{H10}\mathbb{N}(2,2) = \mathrm{D}$ *and Theorem 1.4.1. (There is a solver on the web here:*
   `https://www.alpertron.com.ar/QUAD.HTM`

7. *For all n,* $\mathrm{H10}\mathbb{Z}(2,n) = \mathrm{D}$. *This is a sophisticated theorem due to Siegel [11]. See also Grunewald and Seigel [4].*

4 Discussion

If I was to draw the grid for H10ℕ or H10ℤ mentioned in the introduction there would be a large space of problems that are open. We give an example of a part of that space.

Recall that $\mathrm{H10}\mathbb{Z}(d,1) = \mathrm{D}$, $(\forall n)[\mathrm{H10}\mathbb{Z}(2,n) = \mathrm{D}]$, and $\mathrm{H10}\mathbb{Z}(8,174) = \mathrm{U}$. The folloiwng are unknown:

1. $\mathrm{H10}\mathbb{Z}(3,2), \mathrm{H10}\mathbb{Z}(3,3), \mathrm{H10}\mathbb{Z}(3,4), \ldots$.

2. $\mathrm{H10}\mathbb{Z}(4,2), \mathrm{H10}\mathbb{Z}(4,3), \mathrm{H10}\mathbb{Z}(4,4), \ldots$.

3. $\mathrm{H10}\mathbb{Z}(5,2), \mathrm{H10}\mathbb{Z}(5,3), \mathrm{H10}\mathbb{Z}(5,4), \ldots$.

4. $\mathrm{H10}\mathbb{Z}(6,2), \mathrm{H10}\mathbb{Z}(6,3), \mathrm{H10}\mathbb{Z}(6,4), \ldots$.

5. $\mathrm{H10}\mathbb{Z}(7,2), \mathrm{H10}\mathbb{Z}(7,3), \mathrm{H10}\mathbb{Z}(8,4), \ldots$.

6. $\mathrm{H10}\mathbb{Z}(8,2), \mathrm{H10}\mathbb{Z}(8,3), \mathrm{H10}\mathbb{Z}(8,4), \ldots, \mathrm{H10}\mathbb{Z}(8,173)$.

The situation is worse than it looks. Consider the equation

$$x^3 + y^3 + z^3 = k.$$

It is easy to show that, For $k \equiv 4,5 \pmod 9$, there is no solution in ℤ. What about for $k \not\equiv 4,5 \pmod 9$?

1. Health-Brown [5] conjectured that there were an infinite number of $k \not\equiv 4,5 \pmod 9$ for which there is a solution in ℤ.

2. So far all $0 \le k \le 33$ with $k \not\equiv 4,5 \pmod 9$ there is a solution in ℤ. The case of $k = 33$ was solved by Booker [2] in 2019. This work was rather difficult and required both hard mathematics, clever computer science, and massive computing time.

3. For more on this history of this problem, and some references, see the paper of Booker.

Consider the function that, on input k, determines if $x^3 + y^3 + z^3 = k$ has a solution in $\mathbb{Z}$. Is this function computable? I suspect yes since I cannot imagine coding Turing Machine computations into such a restricted equation. Plus the least n for which there is any $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{U}$ is $\mathrm{H10}\mathbb{Z}(3.2 \times 2^{45}, 20) = \mathrm{U}$.

What is the smallest n such that for some d, $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{U}$? We present an informed opinion by paraphrasing Sun [12] (Page 4):

It is not known if there is a d such that $\mathrm{H10}\mathbb{Z}(d, 3) = \mathrm{U}$. *Baker [1] showed that if* $F(x, y) \in \mathbb{Z}[x, y]$ *is irreducible, homogenous, and of degree* ≥ 3*, then for any* $m \in \mathbb{Z}$ *there is an effective algorithm to find integral solutions of the equation* $F(x, y) = m$*. Baker [1], Matiyasevich and Robinson [10] believed that this is about as far as you can go, in terms of number of variables, and hence there is a d such that* $\mathrm{H10}\mathbb{Z}(d, 3) = \mathrm{U}$.

I have some suggestions and thoughts:

1. Study particular equations such as $x^3 + y^3 + z^3 = k$. I suspect this is already happening.

2. Catalog them so that the open problems are clear.

3. Work on showing $\mathrm{H10}\mathbb{N}(d, n) = \mathrm{U}$ or $\mathrm{H10}\mathbb{Z}(d, n) = \mathrm{U}$ seems to have stalled. Perhaps the problems left are to hard. Perhaps the problems left could be resolved but it would be very messy. Perhaps computer-work could help. Perhaps the problems left are decidable. In any case, there should be an effort in this direction.

5 Acknowledgement

We thank David Marcus for proofreading and commentary.

References

[1] Alan Baker. On the representation of integers by binary forms. *PTRS*, 263:173–191, 1968.

[2] Andrew Booker. Cracking the problem with 33, 2019. `https://arxiv.org/abs/1903.04284`.

[3] Martin Davis, Hillary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Annals of Mathematics*, 74:425–436, 1961.

[4] Grunewald and Siegel. On the integer solutions of quadradic equations. *J. Reine Angew. Math.*, 569:13–45, 2004.

[5] Roger Heath-Brown. The density of zeros of forms for which weak approximation fails. *Mathematics of Computation*, 59(200):612–623, 1992.

[6] James Jones. Universal Diophantine equations. *Journal of Symbolic Logic*, 47(3):549–571, 1982.

[7] Jeffrey Lagarias. Succinct certificates for the solvability of binary quadratic diophantine equations. In *20st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 47–54. IEEE, 1979. `https://arxiv.org/pdf/math/0611209.pdf`.

[8] Yuri Matijasevic. Enumerable sets are diophantine (Russian). *Doklady Academy Nauk, SSSR*, 191:279–282, 1970. Translation in Soviet Math Doklady, Vol 11, 1970.

[9] Yuri Matijasevic. *Hilbert's Tenth Problem*. MIT press, Cambridge, 1993.

[10] Yuri Matijasevic and Julia Robinson. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, pages 521–553, 1975.

[11] Siegel. Zur theoire der quadratischen formen. *Sitzungsberichte der Preusssschen Akademie der Wissenschaften Physicalisch-Mathematische Klasse*, 2:21–46, 1972.

[12] Zhi-Wei Sun. A new relation-combining theorem and its application. *ZL*, 38:209–212, 1992. `http://maths.nju.edu.cn/~zwsun/14z.pdf`.